RSA CONFERENCE ASIA PACIFIC 2013

VULNERABILITY MANAGEMENT AND RESEARCH PENETRATION TESTING OVERVIEW

Len Kleinman
Director ATO Trusted Access
Australian Taxation Office

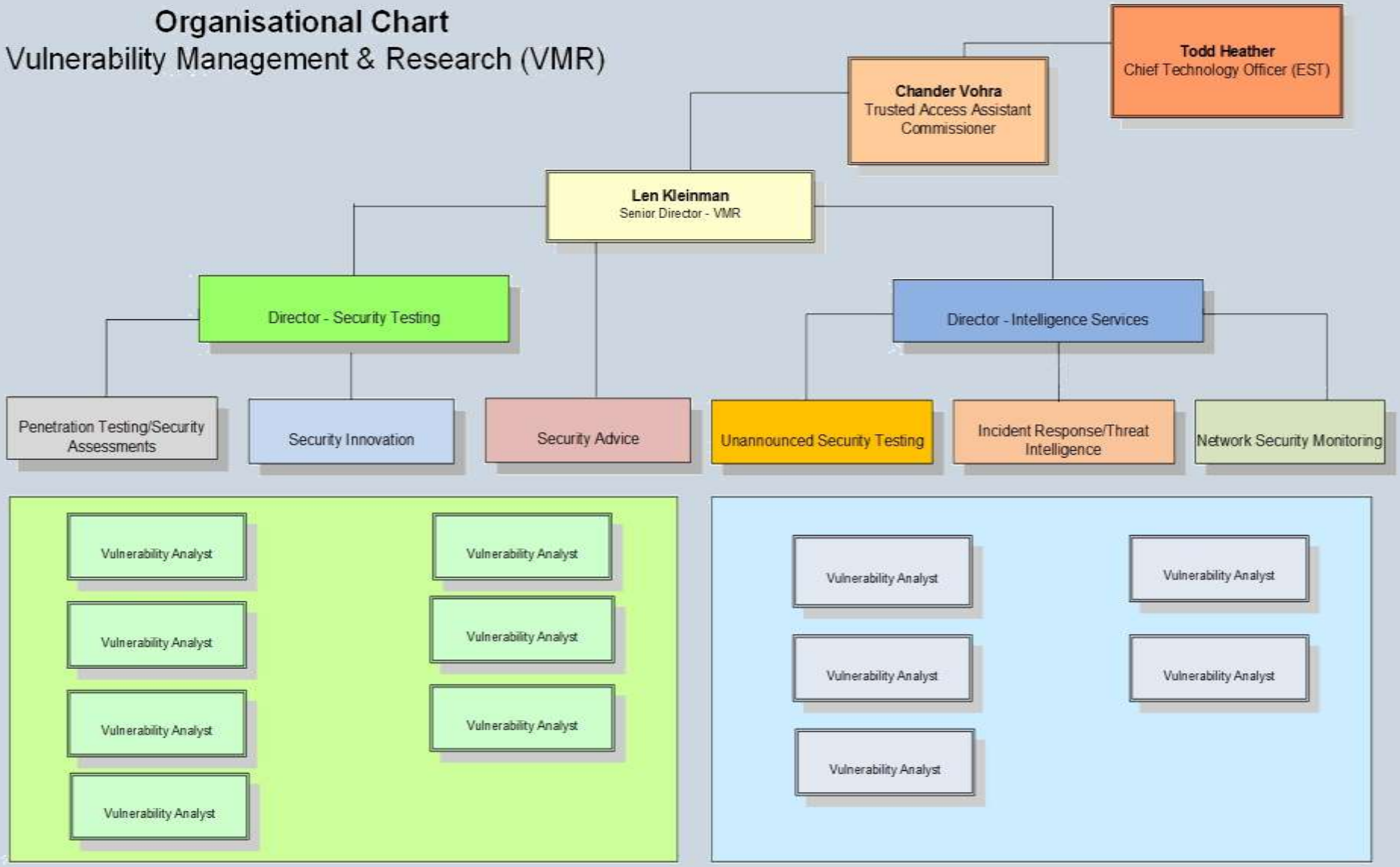
Session ID: DAS-W01
Session Classification: General Interest

What is Vulnerability Management?

"The on-going approach to the collection and analyses of information regarding vulnerabilities, exploits and possible inappropriate communications in identifying the level of IT risk the ATO may be facing at any one instant in time."

Vulnerability Centric – Evidence based

Organisational Chart
Vulnerability Management & Research (VMR)



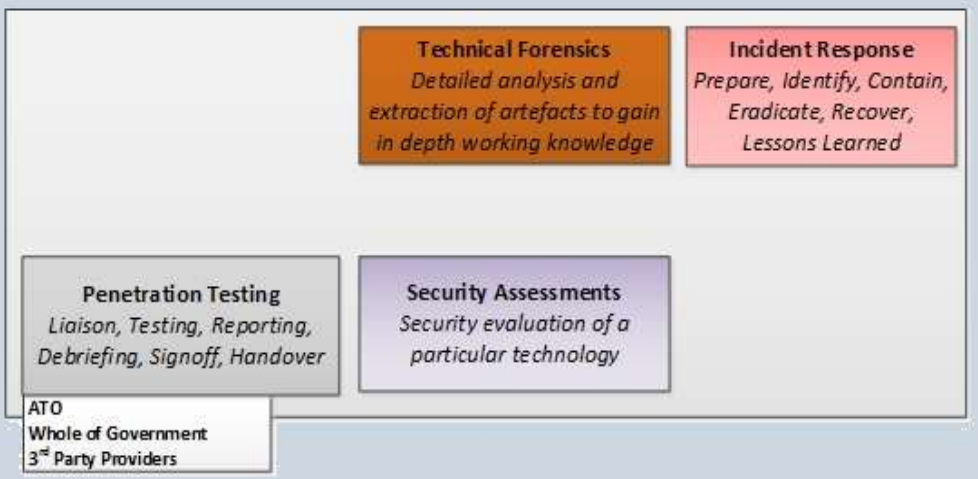
Team Skills/Qualifications

- Master of Information System Security
- Master of Business Administration (In Progress)
- Master of Computer Science (In Progress)
- Bachelor of Computer Science (with honours)
- Bachelor of Information Technology
- Bachelor of Science (Software Engineering)
- Bachelor of Computer Systems Engineering
- Bachelor of Business Information Systems
- Graduate Diploma Taxation Studies
- Diploma in Information Technology
- SANS GWAPT Web Application Penetration Testing
- SANS GPEN Advanced Network Penetration Testing
- SANS GCIH Certified Hacker Techniques, Exploits and Incident Response
- SANS GAWN Certified Auditing Wireless Networks
- SANS GCFA Certified Forensics Analyst
- SANS GCIA Certified Intrusion Analyst
- SANS GIAC GCUX Certified UNIX Administrator
- SANS GIAC Reverse Engineering Malware
- SANS GXPN Advanced Penetration Testing
- SANS Advanced Web App Pentesting
- Certificate IV in Government
- Certificate IV in Government (Investigations)
- Cisco Certified Network Associate (CCNA)
- Attorney General PSCC Training in IT Security & Security Risk Management
- Cisco Certified Security Associate
- Checkpoint Certified Security Administrator
- Checkpoint Certified Security Expert
- Netwitness Analyst
- Microsoft Certified Security Administrator
- Offensive Security Certified Professional
- Graduate Diploma of Business Mgt.
- Diploma of Security & Risk Mgt.
- Oracle Developer/Designer Certified
- CISSP
- CISA – Certified Information Security Auditor
- Certfied ITIL Service Management
- OSSTM – Open Source Secure Training Manual
- Diploma in Network Engineering
- Cert IV in Network Management
- CEH Certified Ethical Hacker
- IRAP Assessor

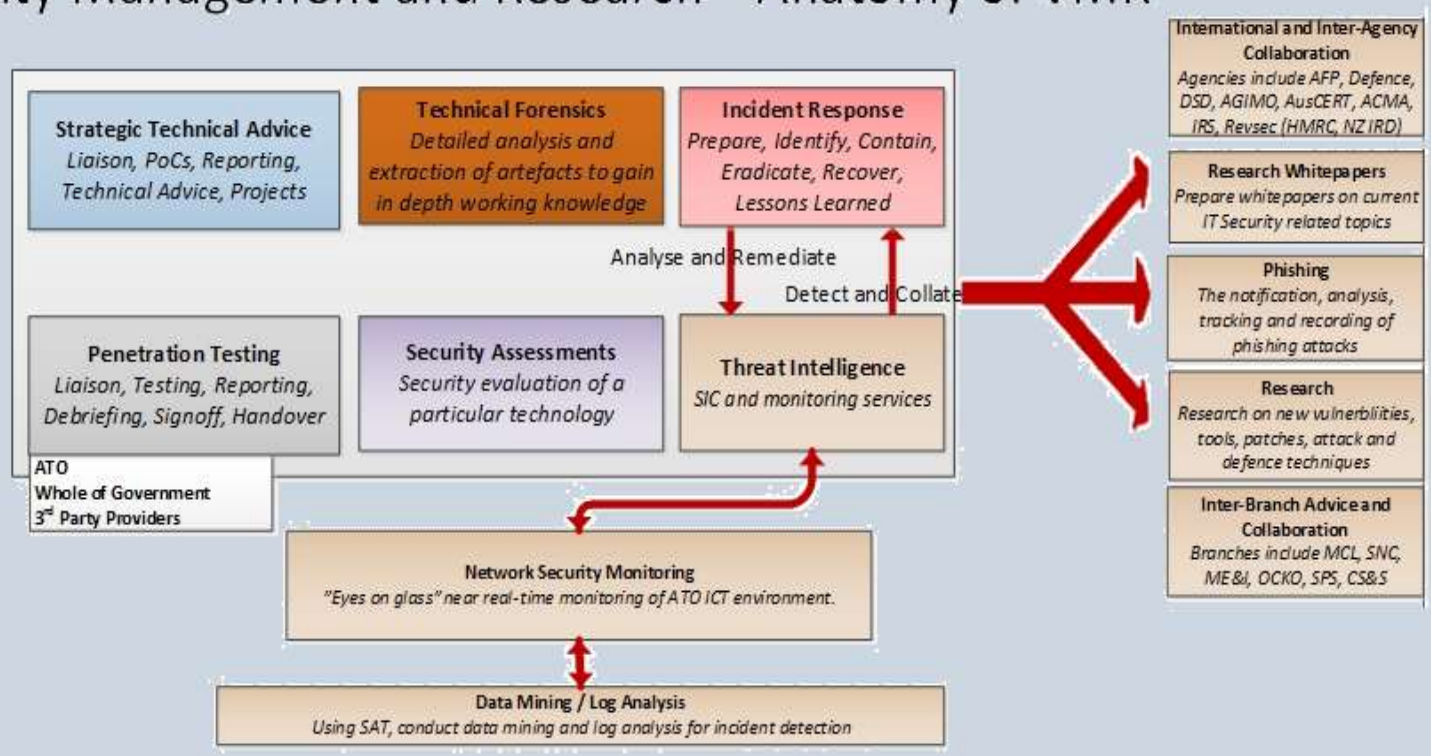
VMR Roles and Responsibilities

- Vulnerability Management :
- Security Testing
  - Penetration Testing
  - Security Assessments
  - Red teaming
  - Production System testing
  - Verification testing
- Threat Intelligence
  - Incident response
  - Monitoring and alerting
- Innovation Development

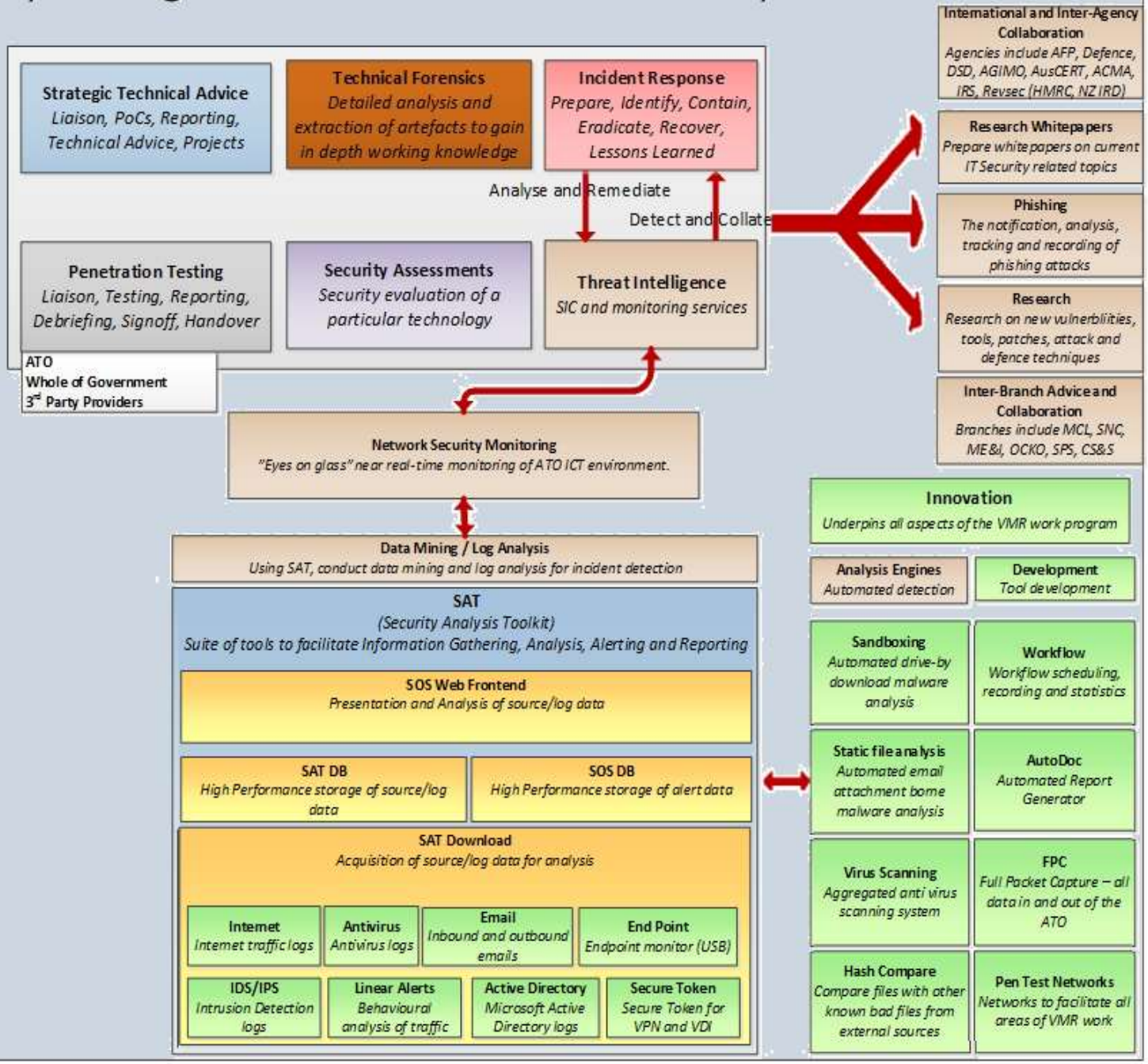
Vulnerability Management and Research – Anatomy of VMR



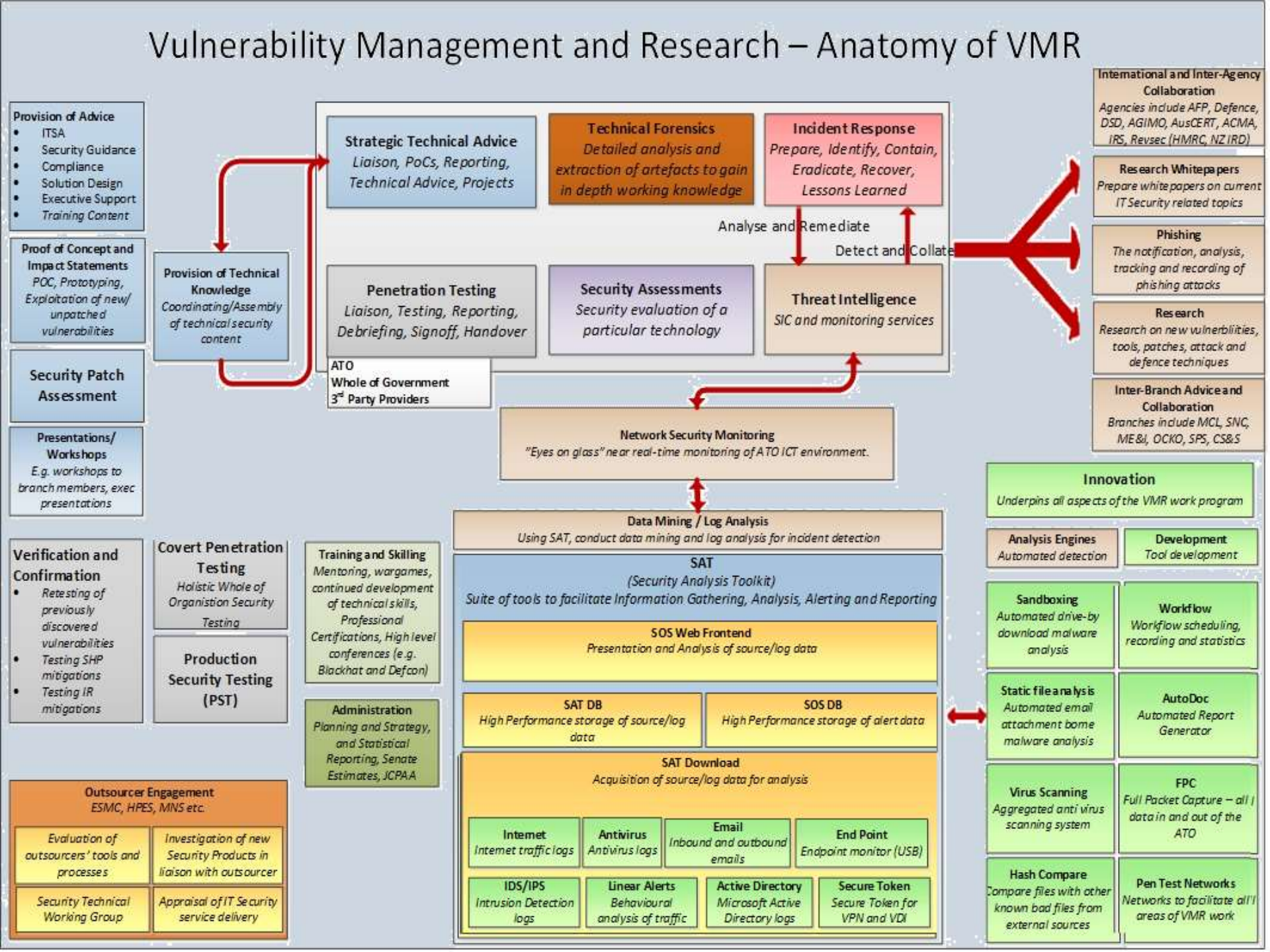
Vulnerability Management and Research – Anatomy of VMR



Vulnerability Management and Research – Anatomy of VMR



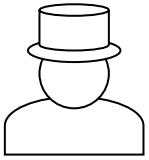
Vulnerability Management and Research – Anatomy of VMR



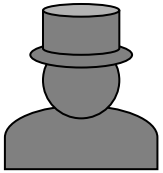
What is a Penetration Tester?

- An Out-of-the-box thinker
- One who bends computers to their will
- What's with the hats?

Black = Cracker, script kiddie



White = Ethical Hacker / Corporate Hacker



Grey = Full disclosure and Hactivist

What **is a Penetration Test?**

"*A program of systematic testing that identifies weaknesses inherent in IT systems. System owners and Security administrators use the results of the testing to improve the security posture of the application/system and therefore improve the overall ATO IT environment.*"

How we developed our capability – The Journey

- Started small – focus was on **reporting** on vulnerabilities
- Decision to develop hands on capability
  - **Application** focus
  - Collaborative effort with a provider
- Applied relevant training and skilling program
- Developed our risk matrix
- Extended scope to include network security testing
- Extended to full system testing as per NIST definition
- Extended function to Red teaming
- Extended function to production systems testing

How we developed our capability – The Journey

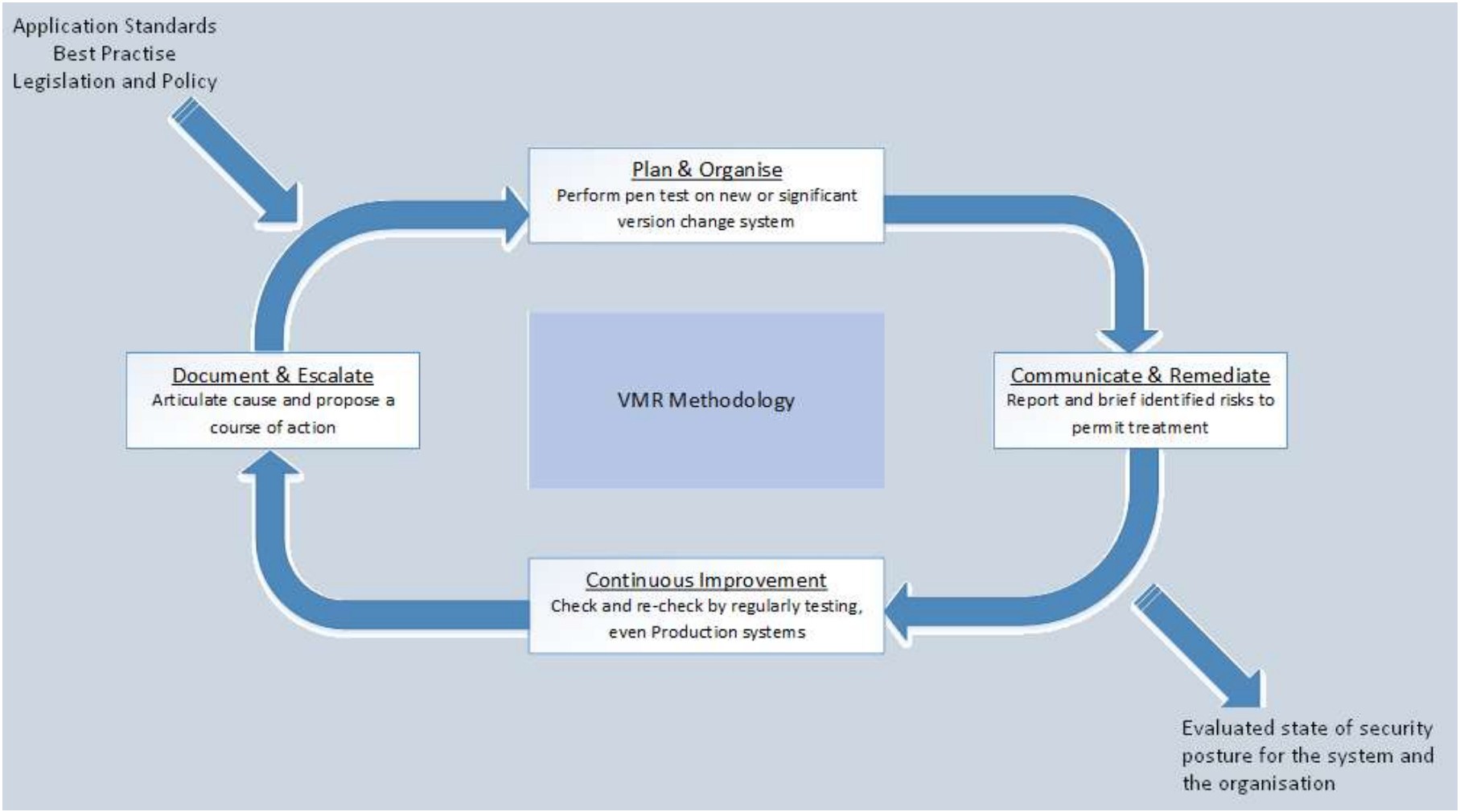
- NIST definition of System NIST SP800-42 Guideline on Network Security Testing:

  System – A system is any of the following:

  + Computer system (e.g., mainframe, minicomputer)
  + Network system (e.g., local area network [LAN])
  + Network domain
  + Host (e.g., a computer system)
  + Network nodes, routers, switches and firewalls
  + Network and/or computer application on each computer system.

How **is a Penetration Test performed?**

- Penetration Test Team coordinates with the project manager
- Client Consensus Statement – Set and manage expectations
- Penetration Test results peer reviewed
- Draft report circulated for review by relevant stakeholders
- Once a Penetration test is finalised, it is approved and signed by:
  - Senior Director VMR
  - The CTO/AC Trusted Access; and
  - The system owner
- VMR conducts de-briefing sessions with the System Owners
  - Flows into the education and compliance aspects
- Any **residual risk** is accepted by the System Owner


Application Standards
Best Practise
Legislation and Policy
Plan & Organise
Perform pen test on new or significant version change system
Communicate & Remediate
Report and brief identified risks to permit treatment
Continuous Improvement
Check and re-check by regularly testing, even Production systems
Document & Escalate
Articulate cause and propose a course of action
VMR Methodology
Evaluated state of security posture for the system and the organisation

VMR's penetration testing is normally conducted in four phases:

Test Phase	Planning and Reconnaissance Phase	Information Gathering. Setting up and setting expectations
	Probing Phase	Vulnerability Identification
	Attack Phase	Exploitation of identified vulnerabilities through penetration Optional - social engineering Optional - physical penetration
Reporting Phase	Detailed reporting on the activities, results and recommendations as a result of testing	

Structure of a Pen Test : Incorporating DREAD model

Consequence	Consequence Description
Insignificant	No injuries, low financial loss
Minor	First aid treatment, on-site release immediately contained, medium financial loss
Moderate	Medical treatment required, on-site release contained with outside assistance, high financial loss
High	Extensive injuries, loss of production capability, off-site release with no detrimental effects, major financial loss
Very High	Death, toxic release off-site with detrimental effect, huge financial loss

CONSEQUENCE

Likelihood	Likelihood Description
Almost certain	Is expected to occur in most circumstances
Likely	Will probably occur in most circumstances
Possible	Might occur at some time
Unlikely	Could occur at some time
Rare	May occur only in exceptional circumstances

LIKELIHOOD

Structure of a Pen Test :

LEVEL OF RISK:

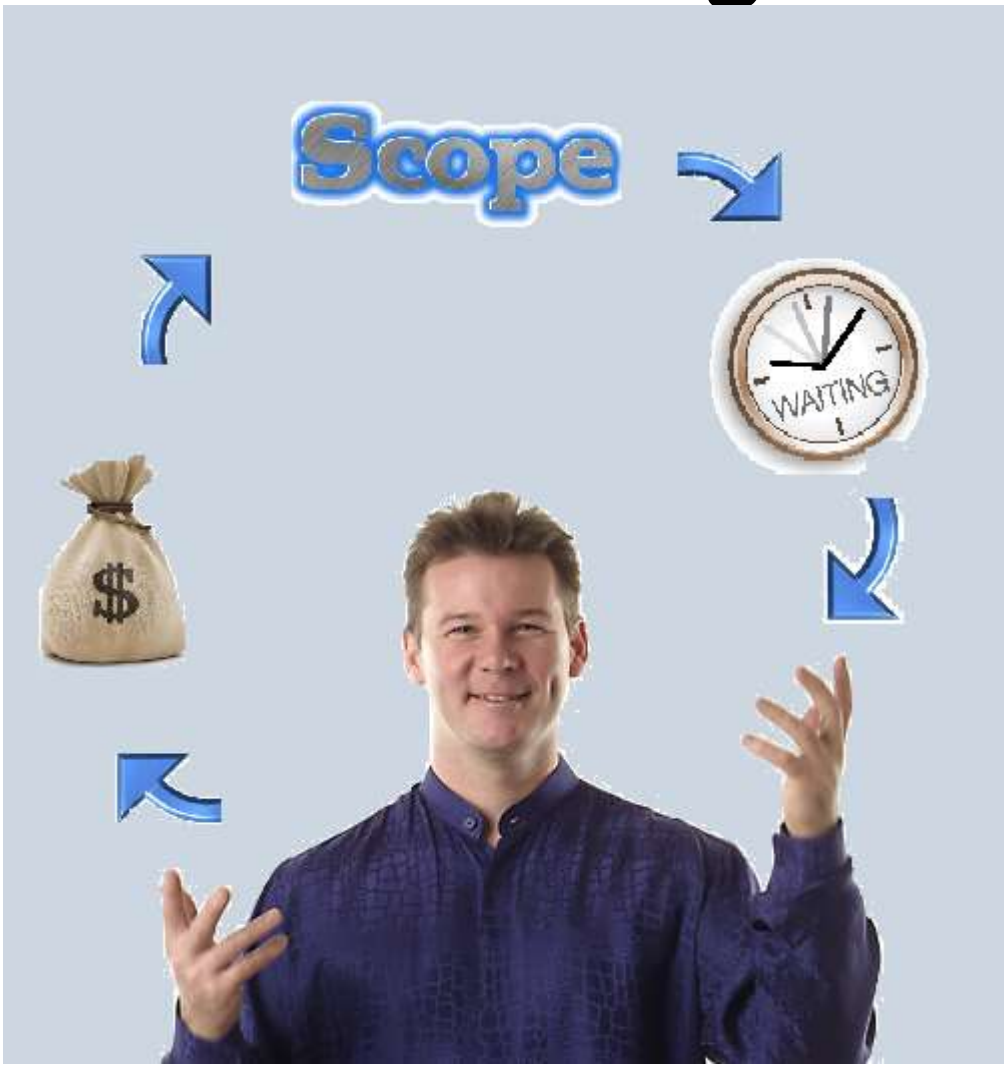
Likelihood	Consequences				
	Insignificant	Minor	Moderate	High	Very High
Almost certain	H	H	E	E	E
Likely	M	H	H	E	E
Possible	L	M	H	E	E
Unlikely	L	L	M	H	E
Rare	L	L	M	H	H

E: extreme risk; immediate action required
H: high risk; senior management attention needed
M: moderate risk; management responsibility must be specified
L: low risk; manage by routine procedures

Salient Points of Interest

- Diversity and variety is very important
  - Rotation within the team.
- Early notification
  - Don’t do it!
- “Mini” pen test
  - No such thing. Do they mean a vulnerability scan?
- Verification test
  - Do not accept in blind faith.
  - Prepare for the growth.
- Recruit appropriately.

The Challenge:



What is it good for? The “Value” component

- Tests exposure of **known** security threats and vulnerabilities to both internal and external attack
- Provides a **snapshot** in time of what security looks like. Sets a benchmark.
- Assesses monitoring and **escalation** procedures.
- Provide advice, solutions and recommendations to enhance the ATO’s security posture at both the **enterprise** and/or **process** level.

What are the benefits? The “Value” Component

- Improved information security knowledge and understanding around the **real** threats and **vulnerabilities** in ATO systems and processes.
- Proactive identification of potential **risk** and provision of assistance in mitigating these risk immediately.
- Assist in the decision making process e.g. Go Live!
- Education opportunity, ….BUT
  - Only for those who want and can be educated.

Problems, Issues and Concerning Observations

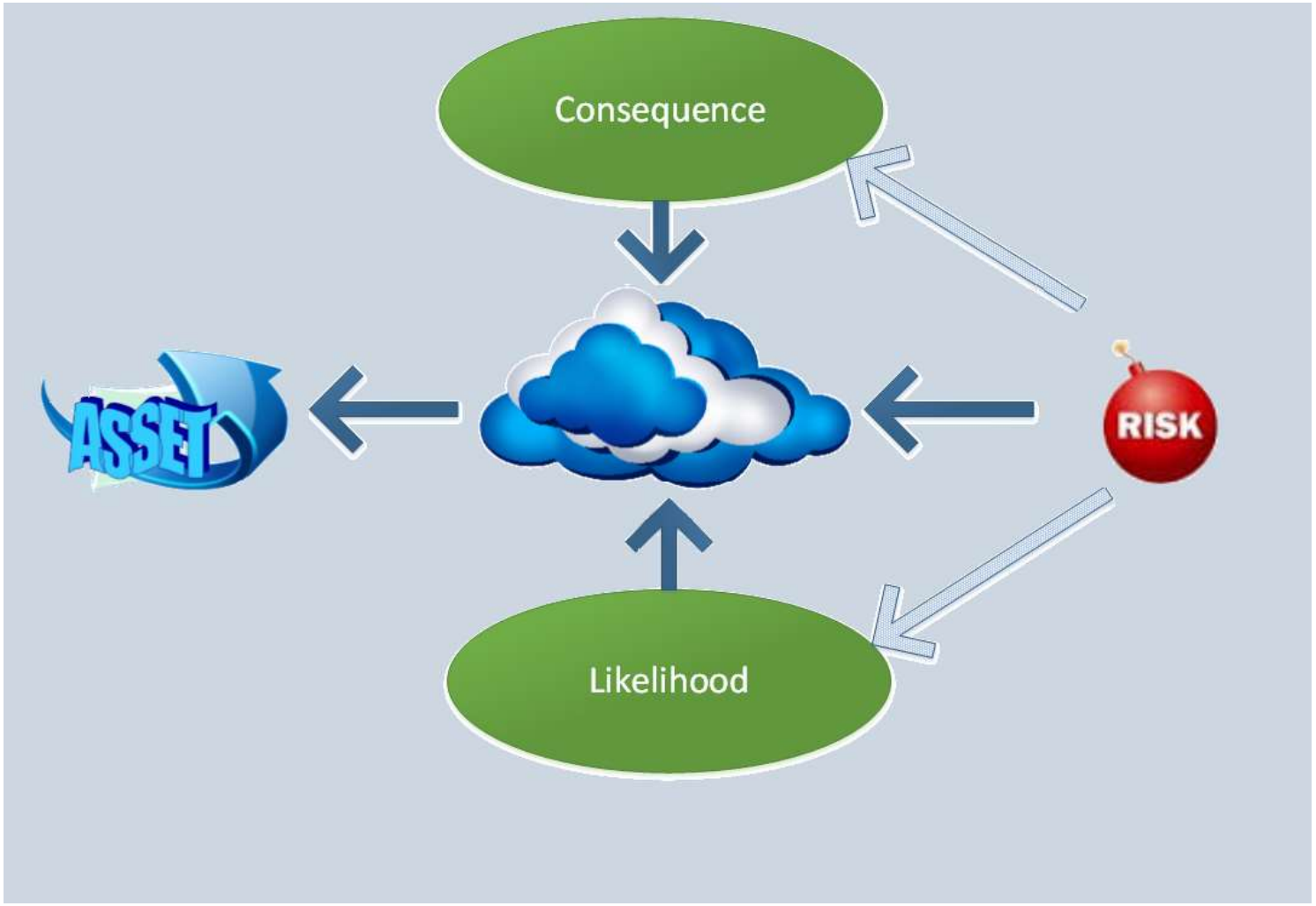
- Too many **Generalist** playing in the **specialist** space.
  - Everybody wants in!
  - Terminology matters.
- Increasing sophistication of attacks.
- Is **not** assurance/compliance/audit work – It can be part of a program where level of assurance is derived from an interpretation of the results. Assurance is subjective.
- Scoping http://risky.biz/news_and_opinion/metlstorm/2009-04-14/poor-scoping-disastrous-security
- Massive gap in technical understanding by persons in a position of responsibility and accountability.

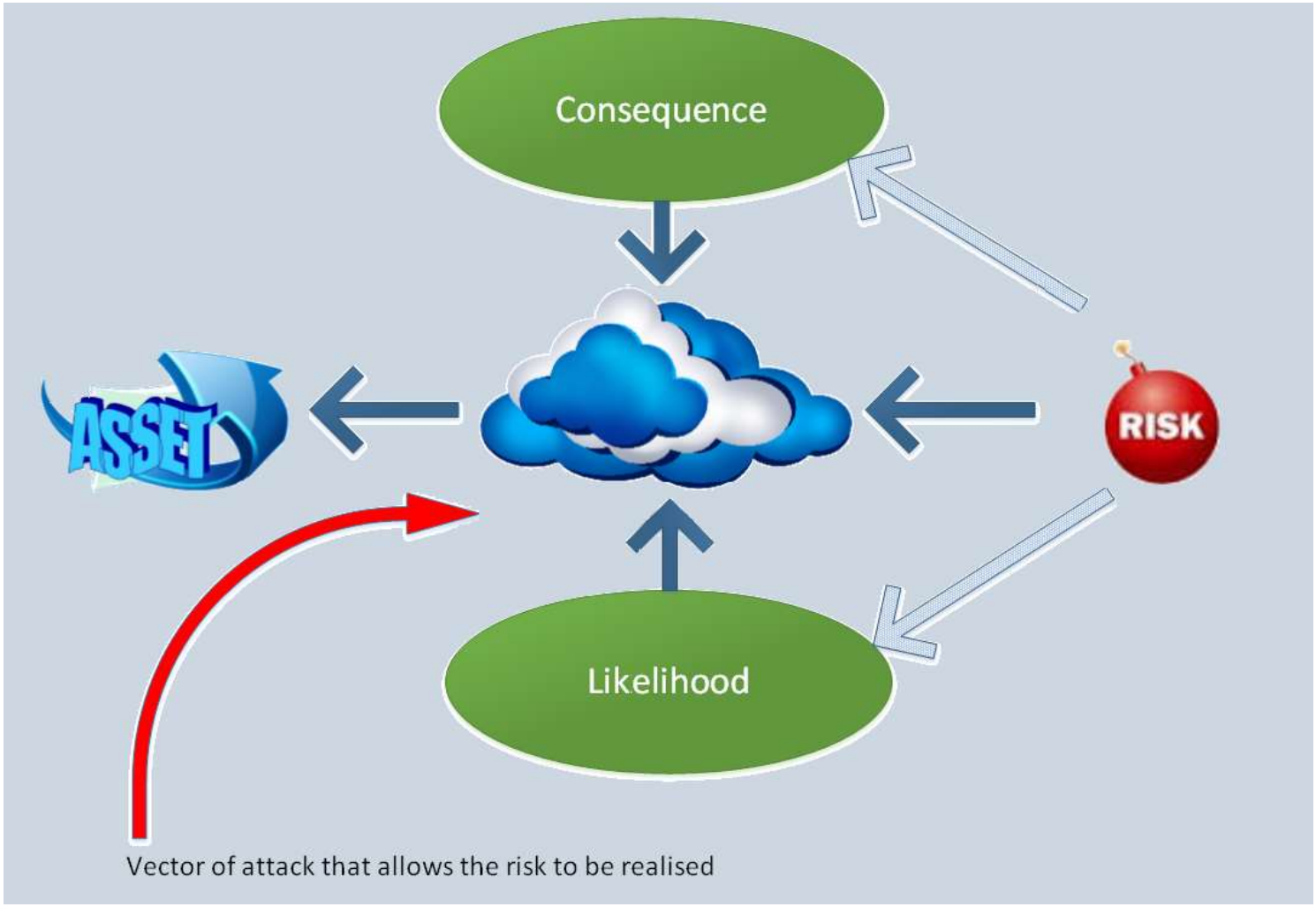

ASSET


ASSET


RISK


ASSET
RISK


Consequence
ASSET
RISK
Likelihood


Consequence
ASSET
RISK
Likelihood
Vector of attack that allows the risk to be realised

Takeaways

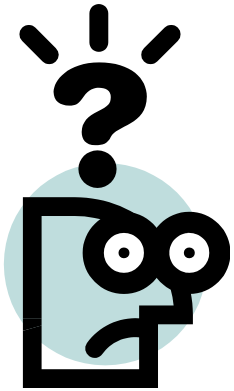
- ✓ Have a thorough documented methodology.
- ✓ Ensure you can articulate the “value”.
- ✓ Quality of Results = methodology + skill + reporting
  - ➢ Clear reporting = ability to remediate.
- ✓ No substitute for capable, qualified, compatible staff.
- ✓ Hands on Testing cost more then “check-box testing” but is reflective of reality, cost more i.e. time and money.
- ✓ Volatile environment – increase sophistication of attacks, increased requirement for expertise, increase requirement to maintain skills.

Excuses and cop-outs

- Our expectation is that a penetration test of systems being relocated from X Data Centre to Y Data Centre is unnecessary as these systems are being moved within network boundaries that have been previously tested.
- That vulnerability has always been there therefore…
- “The system was built in 2002 and the secure coding standards being applied are the 2012 standards. Therefore, we will not be fixing the vulnerabilities identified as the standard is after the build date.”

Excuses and cop-outs

- That vulnerability is not within the scope of the XXX application and we should not be held responsible.
- "…their observed vulnerability for cross site scripting is a common website condition, even evident in the current XXX website, and hence there was an expectation set that there would be no change to the XXX Web Site to resolve this."
- "This vulnerability will not be addressed as part of XXX Upgrade, as mentioned in previous updates the vulnerability was via open ports which is a potential vulnerability for all apps."



This presentation was current in 9/5/2013